TRAF

TRANSMITTAL OF APPEAL BRIEF (Large Entity)

Docket No. ITL.0151US

In Re Application Of: **Ronen Chayat**

Application No.	Filing Date	Examiner	Customer No.	Group Art Unit	Confirmation No.
09/364,375	July 30, 1999	Calvin L. Hewitt II	21906	3621	9363

Invention: **Selectively Transmitting Packets**

COMMISSIONER FOR PATENTS:

Transmitted herewith is the Appeal Brief in this application, with respect to the Notice of Appeal filed on:
December 17, 2007

The fee for filing this Appeal Brief is: No fee due. Fee paid 07/18/2007.

☐ A check in the amount of the fee is enclosed.

☐ The Director has already been authorized to charge fees in this application to a Deposit Account.

☒ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment to Deposit Account No. 20-1504. I have enclosed a duplicate copy of this sheet.

☐ Payment by credit card. Form PTO-2038 is attached.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

Signature

Dated: **December 18, 2007**

Timothy N. Trop, Reg. No. 28,994
TROP, PRUNER & HU, P.C.
1616 S. Voss Road, Suite 750
Houston, TX 77057
713/468-8880 [Phone]
713/468-8883 [Fax]

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)] on
December 18, 2007
(Date)

Signature of Person Mailing Correspondence

Nancy Meshkoff

Typed or Printed Name of Person Mailing Correspondence

cc:

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Applicant:	Ronen Chayat	§	Art Unit:	3621
Serial No.:	09/364,375	§	Examiner:	Calvin L. Hewitt, II
Filed:	July 30, 1999	§	Atty Docket:	ITL.0151US (P6593)
For:	Selectively Transmitting Packets	§	Assignee:	Intel Corporation

Mail Stop **Appeal Brief-Patents**
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Date of Deposit: December 18, 2007
I hereby certify under 37 CFR 1.8(a) that this correspondence is being deposited with the United States Postal Service as **first class mail** with sufficient postage on the date indicated above and is addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Nancy Meshkoff

TABLE OF CONTENTS

REAL PARTY IN INTEREST

The real party in interest is the assignee Intel Corporation.

RELATED APPEALS AND INTERFERENCES

None.

STATUS OF CLAIMS

Claims 1-4 (Rejected).

Claim 5 (Canceled).

Claims 6-15 (Rejected).

Claim 16 (Canceled).

Claims 17-26 (Rejected).

Claim 27 (Canceled).

Claims 28-30 (Rejected).

Claims 1-4, 6-15, 17-26, and 28-30 are rejected and are the subject of this Appeal Brief.

STATUS OF AMENDMENTS

All amendments have been entered.

SUMMARY OF CLAIMED SUBJECT MATTER

In the following discussion, the independent claims are read on one of many possible embodiments without limiting the claims:

1. A method for use with a computer system, comprising:

receiving packets of at least two types (spec. at page 9, lines 18-24; Fig. 5, 122);

determining which type of packet takes more time to process (spec. at page 9, line 25-page 10, line 5; Fig. 5, 122);

identifying a packet of a first type that takes more time to process (spec. at page 10, lines 15-20, Fig. 5, 119);

identifying a packet of a second type that takes less time to process (spec. at page 10, lines 6-14, Fig. 5, 117); and

transmitting packets of the second type before packets of the first type (spec. at page 9, lines 18-24).

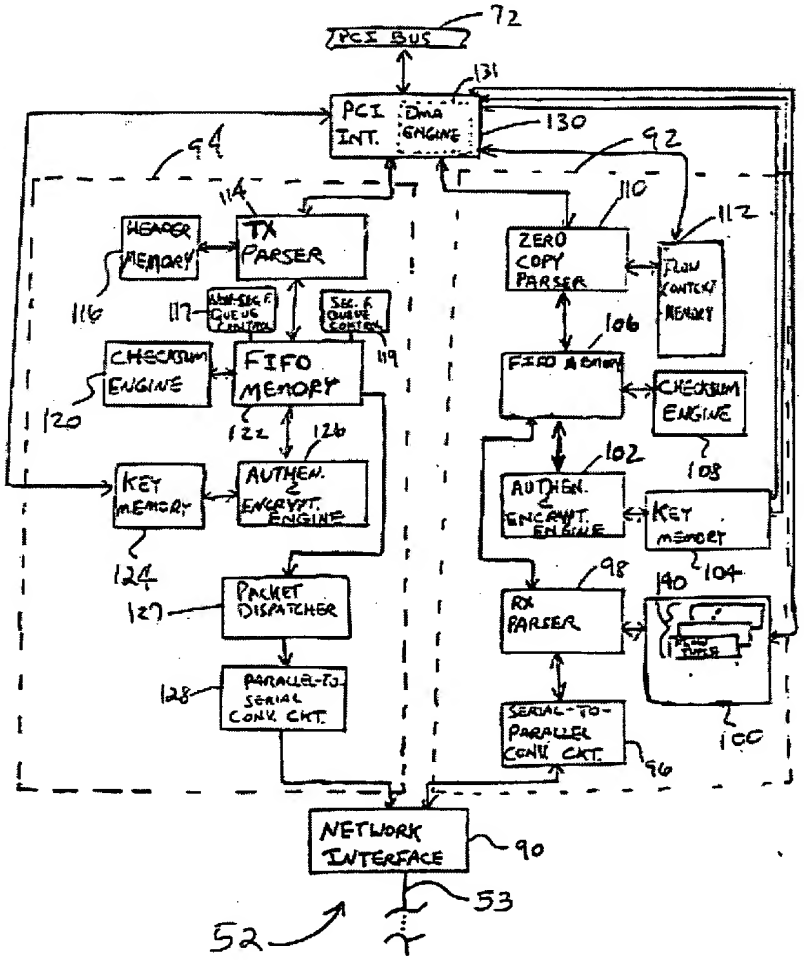

FIG. 5

3. The method of claim 1 including processing said packets in a first in first out memory (spec at page 9, lines 25-29; Fig. 5, 122).

6. The method of claim 1 including receiving packets to be transmitted in a first in first out memory (spec at page 9, lines 25-29; Fig. 5, 122), checking each packet to determine its security status (spec at page 10, lines 6-27; Fig. 5, 117, 119), and providing a pointer to said packet based on its security status (spec at page 10, lines 6-27; Fig. 5, 117, 119).

7. The method of claim 6 including organizing a plurality of packets in said first in first out memory as a linked list of packet blocks (spec at page 10, lines 27-29).

8. The method of claim 7 including marking each of said packet blocks in said first in first out memory as being either a security packet or a non-security packet (spec at page 9, line 29-page 10, line 3).

9. The method of claim 8 including marking packets as security packets or non-security packets depending on the attributes that are indicated in an internet protocol header associated with each packet (spec at page 9, line 29-page 10, line 3).

10. The method of claim 7 including processing a security packet in an authentication and security engine, and then providing a pointer that points to the security packet (spec at page 10, lines 15-20; Fig. 5, 126).

11. The method of claim 10 including selecting between pointers to security packets and non-security packets for transmission of said packets from a network controller to a network interface (spec at page 10, lines 6-27).

12. The method of claim 11 including selecting from among the pointers based on a round robin priority basis (spec at page 10, line 27-page 11, line 4).

13. An article comprising a medium storing instructions that, when executed, enable a processor-based system to:

receive packets of at least two types (spec at page 9, lines 18-24; Fig. 5, 122);

determine which type of packet takes more time to process (spec at page 9, line 25-page 10, line 5; Fig. 5, 122);

identify a packet of a first type that takes more time to process (spec at page 10, lines 15-20, Fig. 5, 119);

identify a packet of a second type that takes less time to process (spec at page 10, lines 6-14, Fig. 5, 117); and

transmitting packets of the second type before packets of the first type (spec at page 9, lines 18-24).

15. The article of claim 13, wherein the instructions, when executed, further enable a processor-based system to monitor an input queue and fetch one type of packet to bypass another type of packet for transmission (spec at page 10, line 29-page 11, line 4).

17. The article of claim 13 wherein the instructions, when executed, further enable a processor-based system to receive packets to be transmitted in a first in first out memory (spec at page 9, lines 25-29; Fig. 5, 122), check each packet to determine its security status (spec at page 10, lines 6-27; Fig. 5, 117, 119) and provide a pointer to the packet based on its security status (spec at page 10, lines 6-27; Fig. 5, 117, 119).

24. A network controller for use with a computer system, comprising:

a transmitter (spec at page 9, lines 3-5; Fig. 5, 94) coupled to receive packets of at least two different types, a first type that takes less time to process than a second type that takes more time to process (spec at page 9, lines 18-24); and

a dispatcher (Fig. 5, 122) adapted to determine that said first type takes less time to process than said second type, to identify a packet of said first type and another packet of said second type, and to transmit packets of said first type before packets of said second type spec at page 10, lines 6-27).

28. The controller of claim 24 including a device adapted to mark packets security packets or non-security packets in said first in first out memory based on attributes indicated in an internet protocol header associated with each packet (spec at page 9, line 29-page 10, line 3).

At this point, no issue has been raised that would suggest that the words in the claims have any meaning other than their ordinary meanings. Nothing in this section should be taken as an indication that any claim term has a meaning other than its ordinary meaning.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A. **Whether claims 3, 6-12, 15, 17-23, 26, and 28-30 are indefinite under 35 U.S.C. § 112, second paragraph for failing to particularly point out and distinctly claim the subject matter of the invention.**

B. **Whether claims 1-4, 6-15, 17-26, and 28-30 are unpatentable under 35 U.S.C. § 103(a) over Cidon (US 5,343,473) in view of Taniguchi (US 6,222,841).**

ARGUMENT

A. Are claims 3, 6-12, 15, 17-23, 26, and 28-30 indefinite under 35 U.S.C. § 112, second paragraph for failing to particularly point out and distinctly claim the subject matter of the invention?

A claim must set out and circumscribe a particular area with a reasonable degree of precision and particularity when read in light of the disclosure as it would be by the artisan. *In re Moore,* 439 F.2d 1232, 1235, 169 U.S.P.Q. 236, 238 (CCPA 1971). Acceptability of the claim language depends on whether one of ordinary skill in the art would understand what is claimed in light of the specification. *Seattle Box Co. v. Industrial Crating & Packing, Inc.,* 731 F.2d 818, 826, 221 U.S.P.Q. 568, 574 (Fed. Cir. 1984).

Certain claims were rejected under § 112 as being indefinite. It is pointed out that claim 2 recites processing packets according to security parameters, while claims 3 and 12 recite executing a priority according to first-in-first-out and round robin rules respectively. Of course, the problem with this rejection is that there is nothing inconsistent between these claims. One could process packets according to security packets and then institute first-in-first-out or round robin as desired. For example, in first-in-first-out processing, a FIFO memory 122 is utilized. In this memory, security and non-security packets may be distinguished and non-security packets may be executed one time, security packets the next time, in a round robin fashion. *See* page 11, lines 1-4. Thus, the round robin priority may select first security, then non-security or vice versa and still be completely consistent with other embodiments which add extra variants on the process. Nothing more is set forth in the rejection to explain it and therefore it is believed that this response fairly meets the limited rejection that was posed in the final rejection. Therefore, reversal would be appropriate.

B. Are claims 1-4, 6-15, 17-26, and 28-30 unpatentable under 35 U.S.C. § 103(a) over Cidon (US 5,343,473) in view of Taniguchi (US 6,222,841)?

Claim 1 calls for determining which of two types of received packets takes more time to process. A packet of a first type to take more time to process is identified and a packet of a second type to take less time to process is identified. The claim calls for transmitting packets of the second type (less time to process) before packets of the first type.

It is noted in the office action that Cidon "do not explicitly recite how priority is assigned." Tanaguchi is no better. Tanaguchi states that packets with priority having the same value as the discrimination boundary level are subjected to filtering discrimination "on the basis of their packet sizes, the number of transmitted bytes, and the value Bpc." Taniguchi, col. 19, lines 3-7. The problem is that he does not say what is done with the recited information. In other words, which packets are abandoned and which ones are actually sent, based on the recited information, is not explained.

While a discrimination is done based on packet size, Cidon does not indicate how the discrimination is done, namely, whether packets with larger packet sizes are abandoned or whether packets with smaller sizes are abandoned.

Therefore, the reference is silent at the point of novelty, necessitating reconsideration. In short, nothing teaches transmitting packets of the second type before packets of the first type.

* * *

Applicant respectfully requests that each of the final rejections be reversed and that the claims subject to this Appeal be allowed to issue.

Respectfully submitted,

Date: December 18, 2007

Timothy N. Trop, Reg. No. 28,994
TROP, PRUNER & HU, P.C.
1616 S. Voss Road, Suite 750
Houston, TX 77057
713/468-8880 [Phone]
713/468-8883 [Fax]

Attorneys for Intel Corporation

CLAIMS APPENDIX

The claims on appeal are:

1. A method for use with a computer system, comprising:
receiving packets of at least two types;
determining which type of packet takes more time to process;
identifying a packet of a first type that takes more time to process;
identifying a packet of a second type that takes less time to process; and
transmitting packets of the second type before packets of the first type.

2. The method of claim 1 wherein said two types of packets include security packets and non-security packets and wherein transmitting packets of one type ahead of packets of the other type involves transmitting non-security packets ahead of packets that are security packets.

3. The method of claim 1 including processing said packets in a first in first out memory.

4. The method of claim 1 including monitoring an input queue and fetching one type of packet to bypass another type of packet for transmission.

6. The method of claim 1 including receiving packets to be transmitted in a first in first out memory, checking each packet to determine its security status, and providing a pointer to said packet based on its security status.

7. The method of claim 6 including organizing a plurality of packets in said first in first out memory as a linked list of packet blocks.

8. The method of claim 7 including marking each of said packet blocks in said first in first out memory as being either a security packet or a non-security packet.

9. The method of claim 8 including marking packets as security packets or non-security packets depending on the attributes that are indicated in an internet protocol header associated with each packet.

10. The method of claim 7 including processing a security packet in an authentication and security engine, and then providing a pointer that points to the security packet.

11. The method of claim 10 including selecting between pointers to security packets and non-security packets for transmission of said packets from a network controller to a network interface.

12. The method of claim 11 including selecting from among the pointers based on a round robin priority basis.

13. An article comprising a medium storing instructions that, when executed, enable a processor-based system to:

receive packets of at least two types;

determine which type of packet takes more time to process;

identify a packet of a first type that takes more time to process;

identify a packet of a second type that takes less time to process; and

transmitting packets of the second type before packets of the first type.

14. The article of claim 13, wherein the instructions, when executed, further enable a processor-based system to transmit non-security packets to be transmitted ahead of security packets.

15. The article of claim 13, wherein the instructions, when executed, further enable a processor-based system to monitor an input queue and fetch one type of packet to bypass another type of packet for transmission.

17. The article of claim 13 wherein the instructions, when executed, further enable a processor-based system to receive packets to be transmitted in a first in first out memory, check each packet to determine its security status and provide a pointer to the packet based on its security status.

18. The article of claim 17 wherein the instructions, when executed, further enable a processor-based system to organize a plurality of packets in a first in first out memory as a linked list of packet blocks.

19. The article of claim 18 wherein the instructions, when executed, further enable a processor-based system to mark each of said packet blocks in said first in first out memory as being either a security packet or a non-security packet.

20. The article of claim 19 wherein the instructions, when executed, further enable a processor-based system to mark packets as security or non-security packets depending on the attributes that are indicated in an internet protocol header associated with each packet.

21. The article of claim 20 wherein the instructions, when executed, further enable a processor-based system to provide a pointer that points to a security packet.

22. The article of claim 21 wherein the instructions, when executed, further enable a processor-based system to provide pointers for non-security packets and to select between pointers to security packets and non-security packets for transmission of said packets.

23. The article of claim 22 wherein the instructions, when executed, further enable a processor-based system to select among pointers based on a round robin priority basis.

24. A network controller for use with a computer system, comprising:

a transmitter coupled to receive packets of at least two different types, a first type that takes less time to process than a second type that takes more time to process; and

a dispatcher adapted to determine that said first type takes less time to process than said second type, to identify a packet of said first type and another packet of said second type, and to transmit packets of said first type before packets of said second type.

25. The controller of claim 24 wherein said two types of packets are security packets and non-security packets.

26. The controller of claim 24 including a first in first out memory adapted to process said packets.

28. The controller of claim 24 including a device adapted to mark packets security packets or non-security packets in said first in first out memory based on attributes indicated in an internet protocol header associated with each packet.

29. The controller of claim 28 including an authentication and security engine, and a device adapted to provide a pointer that points to security or non-security packets.

30. The controller of claim 29 including a dispatcher that selects between pointers to security packets and non-security packets for transmission of said packets from said network controller to a network interface.

EVIDENCE APPENDIX

None.

RELATED PROCEEDINGS APPENDIX

None.